AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Jeremy J. Boissy, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a special agent (SA) with the Federal Bureau of Investigation (FBI) and, as such, I am charged with enforcing all federal laws in all jurisdictions of the United States, its territories, and possessions. I have been employed as an FBI SA since March 2019. I have extensive experience investigating all types of computer crimes including criminal and national security computer intrusions, business email compromise schemes, phishing schemes, and ransomware infections. As an FBI SA I have received extensive training in the investigation of violations of federal and state law. I am currently assigned to the Richmond Division of the FBI where I investigate cyber matters, which include computer-enabled criminal violations relating to computer-enabled fraud designed to induce victims to wire money to criminally controlled bank accounts. I have personally participated in the investigation described below.

2. I make this affidavit in support of a criminal complaint, charging NICOLAE-ADRIAN MĂRGĂRIT ("MĂRGĂRIT") with fraud and related activity in connection with computers, in violation of 18 U.S.C. § 1030(a)(4); wire fraud, in violation of 18 U.S.C. § 1343; conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349; money laundering, in violation of 18 U.S.C. § 1956(a)(1); and conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956(h) (collectively, the "Subject Offenses").

3. This affidavit is being submitted for the limited purpose to show merely that there is sufficient probable cause for the requested arrest warrants and does not set forth all my knowledge about this investigation. I have set forth facts that I believe are sufficient to charge MĂRGĂRIT with the criminal conduct set forth herein.

RELEVANT STATUTORY PROVISIONS

4. **Fraud and Related Activity in Connection with Computers:** 18 U.S.C. § 1030(a)(4) makes it a crime for anyone to "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period."

5. **"Protected Computer":** Under 18 U.S.C. § 1030(e)(2)(B), the term "protected computer" is defined as any computer that "is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."

6. **Wire Fraud:** 18 U.S.C. § 1343 makes it a crime when a person, "having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice . . . "

7. **Conspiracy to Commit Wire Fraud:** 18 U.S.C. § 1349 provides that any person who attempts or conspires to commit [a predicate offense, including wire fraud] shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.

8. **Money Laundering:** 18 U.S.C. § 1956(a)(1) makes it unlawful when a person, knowing that the property involved in a financial transaction represents the proceeds of some

form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity—

(A)(i) with the intent to promote the carrying on of specified unlawful activity; or

* * *

(B) knowing that the transaction is designed in whole or in part--

(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or

(ii) to avoid a transaction reporting requirement under State or Federal law…

For purposes of this paragraph, a financial transaction shall be considered to be one involving the proceeds of "specified unlawful activity" if it is part of a set of parallel or dependent transactions, any one of which involves the proceeds of specified unlawful activity, and all of which are part of a single plan or arrangement.

Additionally, 18 U.S.C. § 1956(a)(2) provides that "[w]hoever transports, transmits, or transfers, or attempts to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States or to a place in the United States from or through a place outside the United States" with the intention described above in 18 U.S.C. § 1956(a)(1)(A)(i) or the knowledge described above in 18 U.S.C. §§ 1956(a)(1)(B)(i) & (ii) is also guilty of money laundering.

9. **Conspiracy to Commit Money Laundering:** Title 18, United States Code, Section 1956(h) states that "[a]ny person who conspires to commit any offense defined in this section or section 1957 shall be subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy."

10. **Specified Unlawful Activity:** The definition of "specified unlawful activity" is given in 18 U.S.C. § 1956(c)(7), which lists several categories of offenses that constitute

"specified unlawful activity." Wire fraud, penalized under 18 U.S.C. § 1343, is included as a "specified unlawful activity" for purposes of money laundering in 18 U.S.C. § 1956(c)(7)(A), which in turn incorporates the list of "racketeering activities" set forth in 18 U.S.C. § 1961(1). Computer fraud and abuse, criminalized under 18 U.S.C. § 1030, is a "specified unlawful activity" pursuant to 18 U.S.C. § 1956(c)(7)(D).

CASE BACKGROUND

11. NICOLAE-ADRIAN MĂRGĂRIT is a member of an international criminal conspiracy with other individuals located in the country of Romania, which has engaged in a variety of criminal activity, to include drug trafficking and cybercrime. MĂRGĂRIT has conducted cybercriminal operations for the group. One such operation was an online retail marketplace scheme. In this scheme, cyber criminals targeted third-party sellers on Amazon that regularly received disbursements from Amazon. Cybercriminals used a variety of techniques and strategies to conduct phishing email operations to harvest victims' credentials (i.e., email address and password) for their Amazon Seller Central accounts. The cybercriminals then used the stolen credentials to log into victim accounts and change financial account information to direct disbursements from Amazon to accounts controlled by the conspiracy.

12. For purposes of venue, Amazon has confirmed with the FBI that all internet traffic for accessing Amazon Seller Central accounts for U.S.-based sellers is routed through an Amazon server located in the Eastern District of Virginia.

13. In this case, rather than changing the victims' payment information to a traditional bank account number, the conspiracy used several Hyperwallet account numbers to receive and move the stolen funds. Hyperwallet is a financial payment service owned by PayPal. Hyperwallet provides payment processing for a diverse collection of global industries.

Hyperwallet enables its merchants (clients) to send payments to their customer base (payees) via virtual accounts and direct transfers. In virtual accounts, payees can choose how they want to withdraw money from Hyperwallet. These options include prepaid cards, Venmo transfers, PayPal transfers, checks, cash pickup, or donations. It is a one-way system; payees cannot load funds into a Hyperwallet account for merchants.

14. In or around November 2020, the FBI began investigating a series of Amazon marketplace account compromises. The initial incident involved an internet merchant located in the Eastern District of Virginia, identified herein as "Seller No. 1," which sells toys on Amazon.com. The owner and CEO of Seller No. 1 determined that the company's Amazon marketplace seller account was compromised and that a bi-weekly disbursement was redirected to an unknown bank account ending in -629. However, Amazon was later able to stop the disbursement and return the funds to Seller No. 1. The attempted losses due to the fraud were $176,469.62.

15. Seller No. 1 received two emails on or about November 17, 2020, sent to their business Gmail address. In the first message, allegedly sent by Seller Notification, seller-notification@www-amazon.com, they were informed that Amazon was unable to verify some of the information provided in their seller account. These emails instructed Seller No. 1 to log into their Amazon Seller Central account, locate the emergency notification section, and to enter a valid phone number. Once this was completed, they were to reply within 24 hours with a confirmation email and they would be sent a verification email to confirm the update as the principal account owner. The Reply-To address for this message was Seller Notification, seller-performance@8cnzvfen-amazon.com.

16. A few minutes later, Seller No. 1 received a message that appeared to be from seller-performance@amazon.com, with the actual address being seller-performance@8cnzvfen-amazon.com. A WHOIS[1] query for this domain at Centralops.net[2] revealed that it resolved to IP address 66.96.147.105, with mail exchanger records indicating that email associated with this address should be directed to Google's email servers[3]. This message thanked Seller No. 1 for their confirmation email and instructed them to click on a "Complete Review" button in the email to confirm the update of their phone number as principal account owner. This button contained an embedded hyperlink that connected to a URL[4] containing subdomain name information that included, in part, "sellercentral.amazn.com-594040.eu." (These subdomain names will be discussed more below.) This URL directed a user to a web address controlled by the conspiracy. These messages were received, and the "Complete Review" button was clicked

---

[1] WHOIS (pronounced "who is"), which stands for "who is responsible for this domain name," is a query and response protocol that is used for querying databases that store an Internet resource's registered users or assignees. These resources include domain names, IP address blocks and autonomous systems, but it is also used for a wider range of other information.

[2] Centralops.net is a website that provides access to several free utilities, including WHOIS, for conducting internet research regarding internet domain names, IP addresses, and email addresses, among other things.

[3] Google permits users to register an email address having a domain name other than "gmail.com" or "google.com" and have Google provide email handling services for that address.

[4] URL is an acronym for "uniform resource locator," colloquially known as a Web address, and is a reference to a resource that specifies its location on a computer network and a mechanism for retrieving it. URLs most commonly reference specific web pages. For example, the URL "https://www.justice.gov" will send a user's web browser to the Department of Justice's main "landing page." The URL "https://www.justice.gov/action-center/report-and-identify-missing-persons" specifies a different webpage on the Department of Justice website for reporting missing persons. URLs may also direct an internet user to a webpage on a server that for practical purposes is not locatable with internet search tools and may appear to be composed largely of seemingly random characters, e.g., "https://www.google.com/url?q=https://sellercentral.amazn.com-095890.eu/ap/en/view?b8fec1c1-1700-445d-a367-60d1cf18fc2a&sa=D&sntz=1&usg=AFQjCNEWDxIrxHYeHppZbpdWNWEIzmheYA."

on, by a Seller No. 1 employee. This November 17, 2020 email to Seller No. 1 provides the basis for the wire fraud charge alleged in Count One of the Criminal Complaint.

Expansion of the Investigation

17. Based upon information provided to investigators by Amazon, the owner of a business located in the Eastern District of Virginia – identified herein as "Seller No. 2" – was interviewed regarding the loss of $8,491.33. Seller No. 2 was also an Amazon seller targeted in the subject phishing scheme. On or about October 29, 2020, the owner received an email to his Gmail address from Seller Notification, seller-performance@2bv5bden-amazon.com. This email was similar in content to the first email received by Seller No. 1, requesting the input of a valid phone number and a confirmation reply message. The owner of Seller No. 2 responded to this email.

18. After responding, the owner received a second email on or about October 29, 2020 from Seller Notification, seller-notification@2bv5bded-amazon.com, requesting that he verify his recent account changes by clicking on a "Begin Verification" button. The owner clicked on this link. The 2bv5bded-amazon.com domain resolved to IP address 66.96.147.105, the same IP address associated with the scheme discussed in paragraph 16 that targeted Seller No. 1. The mail exchanger records for this address were also associated with Google.com. The "Begin Verification" button contained a similar malicious hyperlink designed to phish Seller No. 2's Amazon account credentials. Seller No. 2's Amazon Seller Central account was unlawfully accessed on October 30, 2020, which provides the basis for the computer fraud charge alleged in Count Two of the Criminal Complaint.

19. On or about December 10, 2020, December 17, 2020, and December 22, 2020, the Seller No. 2 owner received three additional emails from the subject(s). Each of these

messages indicated that an issue had been found with Seller No. 2's Amazon Seller Central account and requested a reply to start the verification process. The contents of these messages were similar to the first emails received by both Seller No. 2 and Seller No. 1 and did not include buttons with hyperlinks. The December 10, 2020, and December 17, 2020 messages were allegedly sent from Seller-Notification, seller-notification@www-amazon.com, but the Reply-To addresses for each was seller-performance@1cr4x7en-amazon.com. A WHOIS query at centralops.net revealed that this domain again resolved to 66.96.147.105 with Google.com providing email services. The December 22, 2020 email was also allegedly sent from Seller-Notification, seller-notification@www-amazon.com, but the Reply-To address was seller-performance@8cnzvfen-amazon.com, the same email address used for messages received by Seller No. 1.

20. Using the information connected to the Seller No. 1 and Seller No. 2 account takeovers, Amazon conducted an internal investigation to identify any other seller accounts targeted by the same actors. On January 28, 2021, Amazon provided a referral report to the FBI with identifiers for 622 additional seller accounts that appear to have been accessed by the same perpetrators. Of these accounts, 267 had their financial payment information changed at the time of the report, resulting in approximately $500,000 in additional fraudulent disbursements and over $2.2 million in attempted fraudulent disbursements.

21. Using the data obtained by the Seller No. 1 account, Amazon also provided investigators with certain attributes by which it could identify potentially related incidents. Those attributes included: (1) seller account access from IP address ranges 104.128.112.0–104.128.127.255 and 154.13.53.0—154.13.63.255 ("suspect IP range"); (2) target URLs that would allow the perpetrators to change email settings and view upcoming disbursements; and

(3) account access from a new device not previously used by the legitimate account holder. The perpetrators first accessed the seller's account from one of the IP ranges identified above. The perpetrators then visited the seller's accounts notification section and changed the email address used for account update notifications, often providing a new address that added an "l" to the beginning of the existing address on the account. The perpetrators also accessed the disbursement page, which details the amount and timing of any upcoming disbursements. Ultimately, the perpetrators changed the designated financial account for disbursements so that any future disbursements were paid to the financial account(s) of the subject(s).

22. Both Amazon and the FBI continued their respective investigations since Amazon's January 28, 2021 report. On May 19, 2023, Amazon investigators reported that using the attributes described above, as well as data points exchanged between investigators and Amazon throughout the course of the ongoing investigation, the total losses to Amazon seller victims attributable to this scheme was $1,669,429.82, with an additional total recalled disbursements of $274,753.64 and total cancelled disbursements of $3,424,876.52. The aggregate amount of actual and attempted losses was thus $5,369,059.98.

23. In reviewing the account activity described above, the investigation revealed that the perpetrators often accessed and made changes to the seller accounts from AWS-hosted EC2 virtual machines. Each EC2 "instance" [5] is associated with an AWS account. In many of those cases, subjects would change information in the seller accounts, including updating financial

[5] One of Amazon Web Service's (AWS) most well-known products is called Amazon Elastic Compute Cloud (EC2) , and offers businesses the ability to run applications on the public cloud. A software "**instance**" is a separate copy of a software application or service that runs on the same infrastructure, typically servers, as other copies. Instances are created by duplicating the application's data and configurations, which allows multiple users to interact with the software independently.

account information, from the vantage point of the AWS services to avoid suspicious activity detection. The below sections provide details on the subjects' AWS accounts identified to date, many of which were closed for non-payment. Amazon preserved network traffic and 121 instances connected to AWS accounts 619554062742 and 169587936196.

Account Compromises via Amazon EC2 Instances

24. Much of the subject's AWS activity was traced to AWS account 619554062742, which was opened on or about October 20, 2020. Amazon provided the following subscriber information for this account:

AWS Account: 619554062742 ("AWS Account No. 1")
Email: roxanac2020@protonmail.com
Registered Name: roxanac2020
Account registered on: October 20, 2020
Account closed on: January 26, 2021
Phone: +40 757297823 (RO)
Billing address: RO, Ilfov, Magurele, Alunis 59, 077125, Romania
Debit cards:

- 4256031149608984, account holder SANDU ROXANA COSTINA, issued by ING Bank N.V. Romania
- 4256031155538935, account holder SANDU ROXANA COSTINA, issued by ING Bank N.V. Romania
- 5275294800107845, account holder SANDU ROXANA COSTINA, issued by OTP Bank Romania S.A

According to Amazon, the subjects using AWS Account No. 1 launched 397 separate EC2 instances with Microsoft Windows operating systems (i.e., virtual Windows machines) and used those instances to access the Amazon seller accounts at issue and avoid suspicious activity detection on Amazon's infrastructure.

25. For example, the seller account for Seller No. 2 was accessed from IP 154.13.62.141 (within the suspect IP range) on or about October 30, 2020, wherein the account's notification preferences were changed, and the payment account accessed. The account was then accessed approximately four more times subsequently within a two-minute span from AWS

Account No. 1. Ultimately, the subjects obtained a fraudulent disbursement of $8,491.33 on or about November 10, 2020, to a Hyperwallet account with account number ending in 2790.

26. The investigation further revealed that the owner of Amazon Seller No. 3 received an email from seller-performance@1cr4x7en-amazon.com on February 11, 2021, stating that he was required to update his contact settings on his Amazon marketplace account or risk losing access to the platform. The email address seller-performance@1cr4x7en-amazon.com was the same address used to send a similar message to Seller No. 2. On February 11, 2021, the Seller No. 3 owner responded to the email stating that he updated his account. Records from Amazon indicate that on February 12, 2021, Seller No. 3's profile was accessed by IP address 154.13.55.109 (AWS Account No. 1) three times over the course of two minutes. This IP address was part of the same suspect IP range used in the Seller No. 2 compromise. Records from Amazon further indicate that the attacking IP accessed the profile's payment account section. On February 18, 2021, Amazon sent a disbursement to a Hyperwallet account with account number ending in 5617 in the amount of $29,126.53.

27. Further information provided by Amazon revealed that the owner of Amazon Seller No. 4 also had her account's payment section accessed by attacking IP address 154.13.53.12 (AWS Account No.1) over the course of two minutes on September 23, 2020. Records from Amazon further indicate that on November 6, 2020, November 20, 2020, and December 4, 2020, Amazon disbursed $17,833.81, $23,494.55, and $49,118.43 respectively to a Hyperwallet account with account number ending in 1848. This IP address was part of the same attacking range in the Seller No. 2 and Seller No. 3 compromises.

28. The subjects generally connected to AWS Account No. 1 from IP addresses associated with known VPN[6] services. However, some December 2020 and January 2021 connections were made from IP address 185.53.199.131, which public records associate with a Romanian internet service provider, Orange Romania S.A.

29. On or about January 4, 2021, AWS account 169587936196 was registered with the name "roxanacostina22." This account shared a debit card and billing address with the AWS Account No. 1 described above. This account was also accessed from IP address 185.53.199.131. The complete customer details are below:

AWS Account: 169587936196 (AWS Account No. 2)
Email: roxanacostina22@protonmail.com
Registered Name: roxanacostina22
Account registered on: January 4, 2021
Phone: +40 755397643 (RO)
Billing address: RO, Ilfov, Magurele, Alunis 59, 077125, Romania
Debit card: 5275294800107845, account holder ROXANA COSTINA, issued by OTP Bank Romania S.A

Additional AWS Accounts Associated with AWS Accounts 1 and 2

30. Using data for AWS Accounts No. 1 and No. 2, the investigation revealed six other AWS accounts of interest that were likely controlled by the same individual. These accounts were connected by the same debit cards, card holder names, phone numbers, and/or billing addresses. These accounts were also used to launch at least 806 EC2 instances with Microsoft Windows operating systems between December 11, 2019, and October 23, 2020. Below are the customer details for these accounts:

AWS Account: 723015188175 (AWS Account No. 3)
Email: ROXANACOSTINA@protonmail.com

[6] A VPN, or virtual private network, is a service that encrypts a user's internet connection to protect their privacy and security. A VPN masks the true IP address of a user accessing a particular website or service and encrypts the connection so that it cannot be intercepted and eavesdropped upon.

Registered name: ROXANACOSTINA
Account registered on: September 9, 2020
Account closed on: November 11, 2020
Phone: +40 727571425
Billing address: RO, Ilfov, Magurele, Alunis 59, ZIP 077125, Romania
Debit cards:

- 4256031149608984, account holder SANDU ROXANA COSTINA, issued by ING Bank N.V. Romania
- 4256031171828138, account holder PAVEL DANIEL, issued by ING Bank N.V. Romania

AWS Account: 381237994080 (AWS Account No. 4)
Email: mata82465@hotmail.com:
Registered name: mata82465
Account registered on: November 10, 2020
Account closed on: November 10, 2020
Phone: +44 7496283668
Billing address: GB, Glasgow Lanarkshire 17 Finlay Drive G31 2BD, United Kingdom
Debit cards:

- 4256031171828138, account holder SCOTT WALKER LYONS, issued by ING Bank N.V. Romania
- 4256031180393017, account holder SCOTT WALKER LYONS, issued by ING Bank N.V. Romania
- 4256031155538935, account holder SCOTT WALKER LYONS, issued by ING Bank N.V. Romania
- 4256031149608984, account holder SCOTT WALKER LYONS, issued by ING Bank N.V. Romania

AWS Account: 828411491198 (AWS Account No. 5)
Email: edelmira.salinas.ruiz@gmail.com
Registered name: edelmira2020
Account registered on: September 2, 2020
Account closed on: September 16, 2020
Phone: +40 729767365
Billing address: GB, Beverley, East Yorkshire, 128 Flemingate, 077125, United Kingdom
Debit cards:

- 4256031180393017, account holder EDELMIRA SALINAS RUIZ, issued by ING Bank N.V. Romania

- 5374340007628891, account holder EDELMIRA SALINAS RUIZ, issuing bank unknown.

AWS Account: 084088975645 (AWS Account No. 6)
Email: mata82465@gmail.com
Registered name: mata82465
Account registered on: June 24, 2020
Account closed on: July 12, 2020
Phone: +40 723721483
Billing address: RO, Bucharest, Strada Nufarul Galben 89, 077120, Romania
Debit cards:

- 4026430050767772, account holder 190, issuing bank unknown.
- 5374340007628891, account holder EDELMIRA SALINAS RUIZ, issuing bank unknown.

AWS Account: 336612857999 (AWS Account No. 7)
Email: detreaba112@gmail.com
Registered name: Pavel Daniel
Account registered on: November 12, 2019
Account closed on: November 11, 2020
Phone: +40 752762035
Billing address: RO, Jilava, Str. Toamnei Nr. 28, 077120, Romania
Debit cards:

- 4256031171828138, account holder PAVEL DANIEL, issued by ING Bank N.V.
- 4256031169811781, account holder MANDA SANDEL, issued by ING Bank N.V.
- 4462951002519350, account holder PAVEL DANIEL, issued by Unicredit Tiriac Bank S.A.
- 4462951002427281, account holder VARIA IONUT MARIAN, issued by Unicredit Tiriac Bank S.A.
- 4462951002035928, account holder FLORIAN GHITA, issued by Unicredit Tiriac Bank S.A.

AWS Account: 890661272750 (AWS Account No. 8)
Email: adypv1@gmail.com
Registered name: adypv1
Account registered on: July 30, 2020
Account closed on: August 15, 2020
Phone: +40 727571425
Billing address: RO, Bucharest, Nufarul Galben 89, 077120, Romania
Debit cards:

- 4026430050767772, account holder EDELMIRA SALINAS RUIZ, issuing bank unknown.
- 4256031180393017, account holder NIDELEA DRAGOS, issuing bank unknown.

31. On April 19, 2021, a search warrant was executed for multiple Google email addresses associated with the AWS accounts used by the subject(s) to access the compromised Amazon seller accounts:

- seller-performance@8cnzvfen-amazon.com
- seller-performance@2bv5bden-amazon.com
- seller-performance@1cr4x7en-amazon.com
- edelmira.salina.ruiz@gmail.com
- mata82465@gmail.com
- detreaba112@gmail.com
- adypv1@gmail.com

32. Results from this search warrant were received on or about April 22, 2021. A review of the account information provided by Google revealed that multiple Romanian IP addresses were used to login to these email accounts.

33. A review of the results for the detreaba112@gmail.com account (from AWS Account No. 7) identified a forwarded email with the subject "Backup." The original message was sent by unit3admin@icloud.com, to adypno@gmail.com on January 10, 2021, at 01:16 (UTC -8). The message was forwarded by the adypno@gmail.com account to detreaba112@gmail.com and detreaba112@yahoo.com on January 10, 2021, at 01:17 (UTC -8). Google records for adypno@gmail.com revealed the name on the account as Adrian Nicolae.

34. This email included eight quick response (QR) codes for the Google Authenticator App.[7] These QR codes were subsequently scanned into the Google Authenticator

[7] Google Authenticator is a software-based authenticator that implements two-step verification services. Two-step verification provides stronger security for a Google Account or non-Google account that accepts Google authentication codes. The app generates a six-digit authentication

App by investigators, revealing timed verification codes for 77 accounts. The vast majority of these accounts were for Amazon seller accounts. These 77 accounts included adypno@gmail.com and 16 email accounts that Amazon confirmed were associated with Amazon Seller accounts that had been compromised in this scheme.

35. On September 23, 2021, a U.S. magistrate judge approved three search warrants for information and documentation associated with a total of seven email accounts, including adypno@gmail.com. A review of the search warrant results revealed that adypno@gmail.com received what appeared to be a test email on March 19, 2021, at 18:03:51 UTC, which advised the recipient that there was an issue with their Amazon seller account and that the recipient needed to provide the last four digits of his emergency contact number. The "From" field of the email header suggested that this message was sent from seller-notification@amazonservices.com, but the "Reply-To" address was seller-notification@1cr4x7en-amazon.com. Based on my training and experience, I know that cyber criminals will employ aliases to trick their targets into believing they are sending an email to one address, but are actually sending it to another. One feature of Google's Gmail allows users to use alternate email addresses, which serves as a forwarding email address that a user adds to a user's primary email address. By using an alias email address, received emails will appear to be from the alias email address rather than the primary sending address. As previously mentioned, the seller-notification@1cr4x7en-amazon.com email address was used in the phishing attacks against Seller No. 2, Seller No. 3, and Seller No. 4.

---

code on the user's phone, which is valid for approximately 30 seconds. When logging into their account, users enter both their password and the authentication code displayed on their phone.

36. Subscriber information obtained from Google for email account adypno@gmail.com listed the subscriber for the account as "Adrian Nicolae," with a date of birth of December 4, 1984. The recovery email for this account was listed as mata82465@gmail.com, which is the same email address associated with AWS Account No. 6, as shown above. The creation date for the account was August 29, 2019.

Money Laundering and Conspiracy

37. Once Seller No. 2's Amazon seller central account was compromised and its deposit account changed to the Hyperwallet account ending in 2790, the funds were then transferred through Hyperwallet on or about November 12, 2020, to a Romanian-based ING bank account ending in 5979 in the amount of $8,491.33.

38. In addition to fraudulent funds being transferred to overseas bank accounts, the investigation also revealed multiple individuals acting in concert to avoid fraud detection and facilitate the seamless transfer of funds from the scheme. Search warrant production for the detreaba112@gmail.com account revealed the following email conversation with an account identified as georgenicoloiu16@gmail.com:

> *On Wed, Sep 16, 2020 at 2:17 PM george nicoloiu <georgenicoloiu16@gmail.com> wrote:*
>
> *I will send you something else from the NBG National Bank, around 8 this evening. It is a company registered to a [private] individual and it is very-very old and established. Up to 200 can be done easily.*
>
> *On Wed, Sep 16, 2020 at 2:05 PM Andy Passmore <detreaba112@gmail.com> wrote:*
>
> *Anyway, you are spot-on... because it has not really been working, almost not at all until now. Have a little patience, because it is going to be good.*
>
> *On Wed, Sep 16, 2020 at 3:57 AM george nicoloiu <georgenicoloiu16@gmail.com> wrote:*
>
> *Okay, poppy.*

On Wed, Sep 16, 2020 at 1:46 PM Andy Passmore <detreaba112@gmail.com> wrote:

I am taking care [of it], but I am not rushing like last time... I was looking back, and we sent 700k in a rush and it did not work, because I rushed it. I am doing them nice and slow...
This time I want to stress you out, because you will have no place to get as many accounts as I want to. :))))))

On Tue, Sep 15, 2020 at 12:26 PM george nicoloiu <georgenicoloiu16@gmail.com> wrote:

Maybe you can do something faster, even if it is less, just like that, for starters, do you know what I am saying? We will see what happens, how it is... because as far as I know, those large ones are difficult. 🤔🤔🤦

On Tue, Sep 15, 2020 at 5:30 PM Andy Passmore <detreaba112@gmail.com> wrote:

Okay 😉

On Tue, Sep 15, 2020 at 7:25 AM george nicoloiu <georgenicoloiu16@gmail.com> wrote:

PIREUS BANK

SWIFT CODE
PIRBGRAA
IBAN:
GR32 0172 1870 0051 8709 9484 820

ION MARIN KAI YIOS EE (the name of the company)
DOMIKA YLIKA (what the company does)

Up to 300

39. According to records obtained by Hyperwallet and Amazon, the Greece-based Pireus account ending in 4820 shown above received an approximate total of $171,885.27 from six different amazon seller accounts between November 12, 2020, and November 30, 2020.

40. Records obtained from Hyperwallet showed that Hyperwallet accounts were used to transfer funds intended for Amazon sellers to accounts controlled by MĂRGĂRIT's conspiracy from at least September 30, 2020, through September 12, 2022. This provides the

date range for the money laundering conspiracy charge alleged in Count Three of the Criminal Complaint.

Romanian Law Enforcement Investigation

41. On May 5, 2020, Stefan Balaban, a prosecutor at the Valcea regional office in Romania for the Directorate for Investigating Organized Crime and Terrorism (DIICOT), sent a letter requesting FBI assistance with DIICOT BT Valcea's investigations of criminal organized crime groups involved in computer fraud, computer forgery, and money laundering. According to this request, the subjects of these cases aimed to create and control bank financial flows by opening numerous bank accounts abroad and in Romania through numerous lower-level members. Organized crime organizations opened these bank accounts for the purpose of receiving fraudulent funds.

42. According to DIICOT, MĂRGĂRIT obtained credentials of Amazon users through phishing activities. Subsequently, he gained unauthorized access to their user accounts and modified payment details, replacing the holder's account with a financial account facilitated by MĂRGĂRIT. As a result, when a good or service offered through Amazon was purchased, the money was sent to the accounts operated by MĂRGĂRIT's group members instead of the legitimate account of the Amazon seller. DIICOT further indicated that the proceeds from these cybercrimes were invested into activities of international trafficking of cocaine and cannabis.

NICOLAE-ADRIAN MĂRGĂRIT'S Activities in the Scheme

43. On or about May 28, 2020, DIICOT executed a search and arrest warrant on a residence associated with the organized criminal organization described above. MĂRGĂRIT was also living at the residence at that time. During the execution of the warrants, DIICOT seized a series of devices belonging to MĂRGĂRIT. MĂRGĂRIT was released on his own

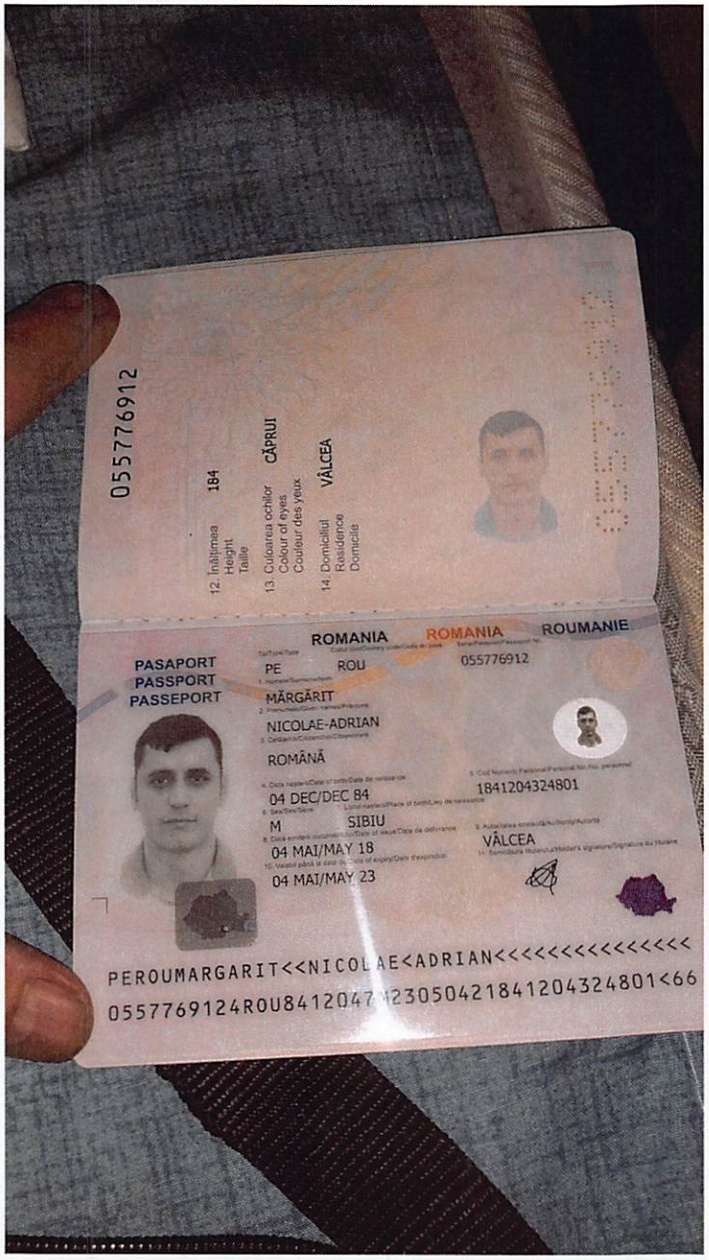
recognizance. Pursuant to a Mutual Legal Assistance Treaty (MLAT CRM-182-86195) request submitted to the Romanian government and dated December 1, 2022, on or about September 24, 2023, the FBI received a hard drive containing data extracted from MĂRGĂRIT's devices by Romanian authorities, including the contents of one laptop, two Samsung Galaxy phones, and one Apple iPhone.

44. Analysis of the computer seized from MĂRGĂRIT by Romanian authorities contained three files named "Y1.doc," "2.doc," and "7.doc." These files appeared to contain victim information and email addresses. Of the email addresses discovered in those three files, Amazon confirmed that at least 27 of them were known victims of the scheme.

45. Analysis of the Random Access Memory (RAM)[8] of the laptop identified a list of approximately 245 unique email addresses present on the machine in emails and files at the time of seizure. Thirty-five of the email addresses were also found in search warrant production from the detreaba112@yahoo.com, detreaba112@gmail.com, seller-notification@8cnzvfen-amazon.com, and seller-notification@2bv5bden-amazon.com accounts; as well as information provided by Amazon. The presence of these emails in the laptop's RAM (as opposed to being information contained in a file saved to the laptop's hard drive), suggests that these addresses had been utilized by the laptop's user or operating system since the laptop had been last powered on.

[8] Random access memory (RAM) is the hardware in a computing device that provides temporary storage for the operating system, software programs and any other data in current use so they're quickly available to the device's processor. Random access memory is considered part of a computer's primary memory. It is much faster to read from and write to than secondary storage, such as hard disk drives (HDDs) or solid-state drives (SSDs). However, RAM is volatile; it retains data only as long as the computer is on. If power is lost, so is the data. When the computer is rebooted, the OS and other files must be reloaded into RAM, usually from an HDD or SSD.

46. Further investigation of the devices provided by Romanian authorities revealed they contained the following two .jpg files depicting the apparent legitimate Romanian passport and Romanian driver's license for MĂRGĂRIT:



47. The date of birth listed on the passport and ID card shown above–December 4, 1984–is the same date of birth listed in subscriber records obtained from Google for the account associated with email address adypno@gmail.com.

48. The FBI conducted a review of IP address information for logins to the below accounts believed to be associated with MĂRGĂRIT:

- adypno@gmail.com
- adypv1@gmail.com
- davidgarcia2020p@gmail.com
- detreaba112@gmail.com
- edelmira.salinas.ruiz@gmail.com
- georgenicoloiu16@gmail.com
- mata82465@gmail.com
- payments@pl-airbnb.com
- razvanclaudiu56@gmail.com
- seller-notification@1cr4x7en-amazon.com
- seller-notification@2bv5bden-amazon.com
- seller-notification@8cnzvfen-amazon.com
- unit3admin@icloud.com

49. A review of the logs to identify which accounts may possibly be controlled by the same actor(s) noted the following activity:

- Between 09:11 UTC and 09:51 UTC on November 28, 2020, the accounts adypv1@gmail.com and mata82465@gmail.com, as well as the Amazon phishing accounts seller-notification@1cr4x7en-amazon.com, seller-notification@2bv5bden-amazon.com, and seller-notification@8cnzvfen-amazon.com, all logged in through IP address 205.251.138.138. Similarly, between 13:36 UTC and 13:41 UTC on December 18, 2020, these same accounts all logged in from IP address 205.251.142.45.

- Between 21:40 UTC and 22:07 UTC on January 15, 2021, the accounts adypno@gmail.com, adypv1@gmail.com, detreaba112@gmail.com, edelmira.salinas.ruiz@gmail.com, mata82465@gmail.com, and payments@pl-airbnb.com, all logged in through IP address 154.29.131.73.

- Between 02:14 UTC and 02:40 UTC on February 22, 2021, the accounts adypno@gmail.com, adypv1@gmail.com, and mata82465@gmail.com, as well as the Amazon phishing accounts seller-notification@1cr4x7en-amazon.com, seller-notification@2bv5bden-amazon.com, and seller-notification@8cnzvfen-amazon.com, all logged in through IP address 154.21.114.159.

- Between 04:01 UTC and 04:10 UTC on March 7, 2021, the accounts adypno@gmail.com, adypv1@gmail.com, and mata82465@gmail.com, as well as the Amazon phishing accounts seller-notification@1cr4x7en-amazon.com, seller-notification@2bv5bden-amazon.com, and seller-notification@8cnzvfen-amazon.com,

all logged in through IP address 154.21.22.60.

- Between 15:10 UTC and 15:42 UTC on April 13, 2021, the accounts adypv1@gmail.com, detreaba112@gmail.com, and payments@pl-airbnb.com, as well as the Amazon phishing accounts seller-notification@1cr4x7en-amazon.com, seller-notification@2bv5bden-amazon.com, and seller-notification@8cnzvfen-amazon.com, all logged in through IP address 38.70.11.207.

The login information to the email accounts from the same IP address in brief time spans strongly suggests that the same user controlled all of the accounts. Because MARGARIT was the account holder for several of the above accounts, it is more than likely he controlled all of the above.

Discovery of CGI Proxy Script and its Modifications

50. The examination of the laptop seized from MARGARIT by Romanian authorities in 2020 revealed that someone, presumably MARGARIT, had modified software to make it appear to his victims that they were inputting their user credentials into Amazon's web page but in fact MARGARIT was harvesting the victims' user credentials. This was a sophisticated "man in the middle" attack[7] contained in a file on his laptop named "cu.pl."

51. MARGARIT's man-in-the-middle scheme contained in the cu.pl computer file was built using software called CGIProxy. CGIProxy is a publicly available software using the CGI (Common Gateway Interface) protocol that can be used to create a web proxy server that allows users to access websites anonymously. In this way, a CGIProxy server functions similarly to a VPN. In extremely basic terms, when a victim of a MARGARIT's phishing email clicked the "Complete Review" button in the email, instead of being directly routed to the

[7] In computer security, a man-in-the-middle (MITM) attack is a cyberattack where the attacker secretly relays, and possibly alters, the data communication between two parties who believe that they are directly communicating with each other, as the attacker has inserted themselves between the two user parties.

Amazon Seller Central webpage they were first routed through a server controlled by MĂRGĂRIT. As the victims entered the username and password for their Amazon Seller Accounts, MĂRGĂRIT's proxy server captured that information. MĂRGĂRIT's CGIProxy servers were further constructed to send the stolen credentials to bocap@protonmail.com. Google listed this email address as the recovery email address for adypv1@gmail.com; the email account associated with AWS Account No. 8.

52. An FBI computer scientist analyzed the cu.pl file found on MĂRGĂRIT's laptop and determined that standard CGIProxy software had been tailored to execute the above-described Amazon seller phishing scheme. Lines of code included instructions for the stolen user credentials, along with the victims' IP addresses, to be written to a text file named "captured_logs.txt" and then forwarded to bocap@protonmail.com.

53. MĂRGĂRIT's modified CGIProxy program also included instructions to capture the "session cookies"[9] that were transmitted by Amazon back to victims when victims accessed their seller accounts, which would simplify MĂRGĂRIT's ability to later access the victims' accounts. The author of the script defined a new function called "manage_cookies1" that exported cookies to an HTML[10] file in a table with a particular format. The unique order in which the table headers for "manage_cookies1" were defined matched cookie files that were identified in a .zip file attachment to an email discovered in search warrant returns for

[9] A **cookie** is a small data file that a web server sends to a user's device while they are browsing a website. The user's web browser stores the cookie and sends it back to the server each time the user requests a new page from that website. Many cookies are persistent; they will remain on a user's computer even after the web browser is closed. **Session cookies**, also known as transient cookies, are temporary cookies that are deleted when a user closes their browser. Session cookies are used to store user-specific information during a single visit to a website, such as login credentials or items in a shopping cart.

[10] Hypertext Markup Language (HTML) is the standard markup language for documents designed to be displayed in a web browser. It defines the content and structure of web content.

detreaba112@yahoo.com. That attached .zip file contained another file called "cs.html." When viewed in a web browser, cs.html displayed a table with the same unique order of table headers described in the "manage_cookies1" function. Due to the unique order of the table headers, which differed significantly from the original format used by the default version of CGIProxy, this table was likely created by the modified script, cu.pl.

Credential Harvesting Servers

54. Analysis of the phishing emails received by numerous Amazon sellers revealed that these phishing messages each contained a link to an internet domain hosted on servers that were owned, maintained, or controlled by Newfold Digital. The IP addresses for those servers were:

- 162.144.78.100
- 162.144.78.186
- 142.4.2.128
- 192.163.212.109
- 192.163.212.110
- 142.4.0.84
- 142.4.0.45
- 142.4.11.163

55. In April 2023, the FBI served an order issued pursuant to 18 U.S.C. § 2703(d) on Newfold Digital for records and information related to the above servers, and the associated user accounts related to the servers. Based on returns from that order, in May 2023, the FBI obtained a search warrant for the content of the servers.

56. The operating software on these various servers contained substantially similar variations of the CGIProxy script identified on MĂRGĂRIT's computer from 2020. The servers also contained Amazon Seller Central session cookies. In addition, the servers contained many

failed automatic emails with the error message "message has lines too long for transport."[11] containing the IP addresses of victims who had their credentials harvested on certain dates. The subject lines of these failed emails contained naming conventions identical to the naming conventions identified in the CGIProxy script. Apart from these failed messages, evidence in the case indicates that numerous other email messages containing harvested Amazon seller account logon credentials were successfully transported to email addresses controlled by or accessible to MĂRGĂRIT.

57. Server statistic files revealed over 170 fraudulent Amazon Seller Central subdomains had been hosted on the servers. This reveals that multiple subdomains were used to phish Amazon sellers, such as sellercentral.amazn.com-594040.eu and sellercentral.amazn.com-492950.eu[12], which were each used to victimize Seller No. 1.

58. The above evidence indicates, then, that the leased Newfold Digital servers were the principal infrastructure that MĂRGĂRIT used to host and execute his CGIProxy man-in-the-middle phishing scheme. In this case, the victims logged into a webpage that looked nearly identical to the actual Amazon Seller Central portal. The victims' login credentials, session cookies, and IP addresses were logged by the servers without the victims being made aware.

---

[11]The failure message "message has lines too long for transport" is an error that usually happens when a sender is trying to send any email or message that exceeds the required line length allowed by the email server or transport protocol being used. Normally, email servers or clients set a limit of words and characters per line.

[12] These subdomains constituted part of the URLs, hidden under the "Complete Reply" button in the phishing emails, that routed victims to MĂRGĂRIT'S phishing servers, such as the bolded section in the following phishing email URL: https://www.google.com/url?q=https://**sellercentral.amazn.com-095890.eu**/ap/en/view?b8fec1c1-1700-445d-a367-60d1cf18fc2a&sa=D&sntz=1&usg=AFQjCNEWDxIrxHYeHppZbpdWNWEIzmheYA.

Romanian Authorities Arrest NICOLAE ADRIAN MĂRGĂRIT

59. On or about September 26, 2023, Romanian Chief Prosecutor Stefan Balaban notified the FBI that DIICOT had arrested NICOLAE ADRIAN MĂRGĂRIT that same day. At the time of MĂRGĂRIT's arrest, DIICOT seized a laptop computer, thumb drive, and three smart phones from him. Upon this notification, FBI investigators then provided Romanian authorities a supplemental MLAT request for the additional devices. On May 29, 2024, Richmond Division received the requested items.

Analysis of Supplemental MLAT Evidence

60. Analysis of the laptop computer's Microsoft Edge browser history revealed that the computer had been used to navigate to and access the Newfold Digital phishing servers. In addition, the browser history revealed a search had been conducted for setting up a hidden VeraCrypt[11] volume[13]. VeraCrypt was also found to be present in the computer's "Downloads" folder. A forensic examination of the laptop revealed over 900GB of disk space that was filled with data that appeared to be encrypted, which would be consistent with the existence of an active VeraCrypt volume on MĂRGĂRIT's laptop.

61. A review of data extracted from a Samsung Galaxy cell phone seized from MĂRGĂRIT revealed that the default time zone setting on the device was to Bucharest, Romania. The phone contained five session cookies associated with the domain amazon.com.

---

[11] VeraCrypt is a free and open-source utility for computer data encryption. Encryption is the process of protecting information or data by using mathematical models to scramble it in such a way that only the parties who have the key to unscramble it can access it. The VeraCrypt software can create a virtual encrypted disk that works just like a regular disk but within a file.

[13] A hard drive "volume" is a logical storage area on a physical disk (e.g., hard drive) that is used to store files, directories, and other data. Volumes are also known as logical drives. Volumes are logically distinct from the physical disk and are treated as separate units by the operating system. Each volume has its own file system, and they can have their own encryption and permissions that are distinct from those of the main hard drive.

Three of these cookies were created on February 3, 2023, and two of the cookies were created on January 2, 2023. The phone also contained nine emails associated with Amazon Seller Central addresses, bearing substantial similarities to the fraudulent emails received by victims in the phishing scheme:

- Seller-performance@f2b3en-amazon.com (one email)
- Floriandumitrescu0@gmail.com (three emails)
- Seller-notification@amazonaws.com (four emails)
- Seller-performance@us-east-4-amazon.com (one email)

62. A review of the web browser history from the Samsung Galaxy cell phone also revealed four connections to the credential harvesting servers on January 2, 2023, and three connections to the credential harvesting servers on February 1, 2023.

CONCLUSION

63. Based on the information detailed above, I respectfully submit there is probable cause to charge NICOLAE-ADRIAN MĂRGĂRIT with the federal offenses of fraud and related activity associated with computers, wire fraud, conspiracy to commit wire fraud, money laundering, and conspiracy to commit money laundering.

Respectfully Submitted,

Jeremy J. Boissy
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on NOVEMBER 26, 2024, in Richmond, Virginia.

/s/ MRC
Honorable Mark R. Colombell
United States Magistrate Judge